Cassandra Crossing/ Il collasso delle IA

(557)—Perché un dettaglio tecnico delle false IA sarà decisivo per cambiarne forse il modello di sviluppo, ma certamente quello di…

Cassandra Crossing/ Il collasso delle IA
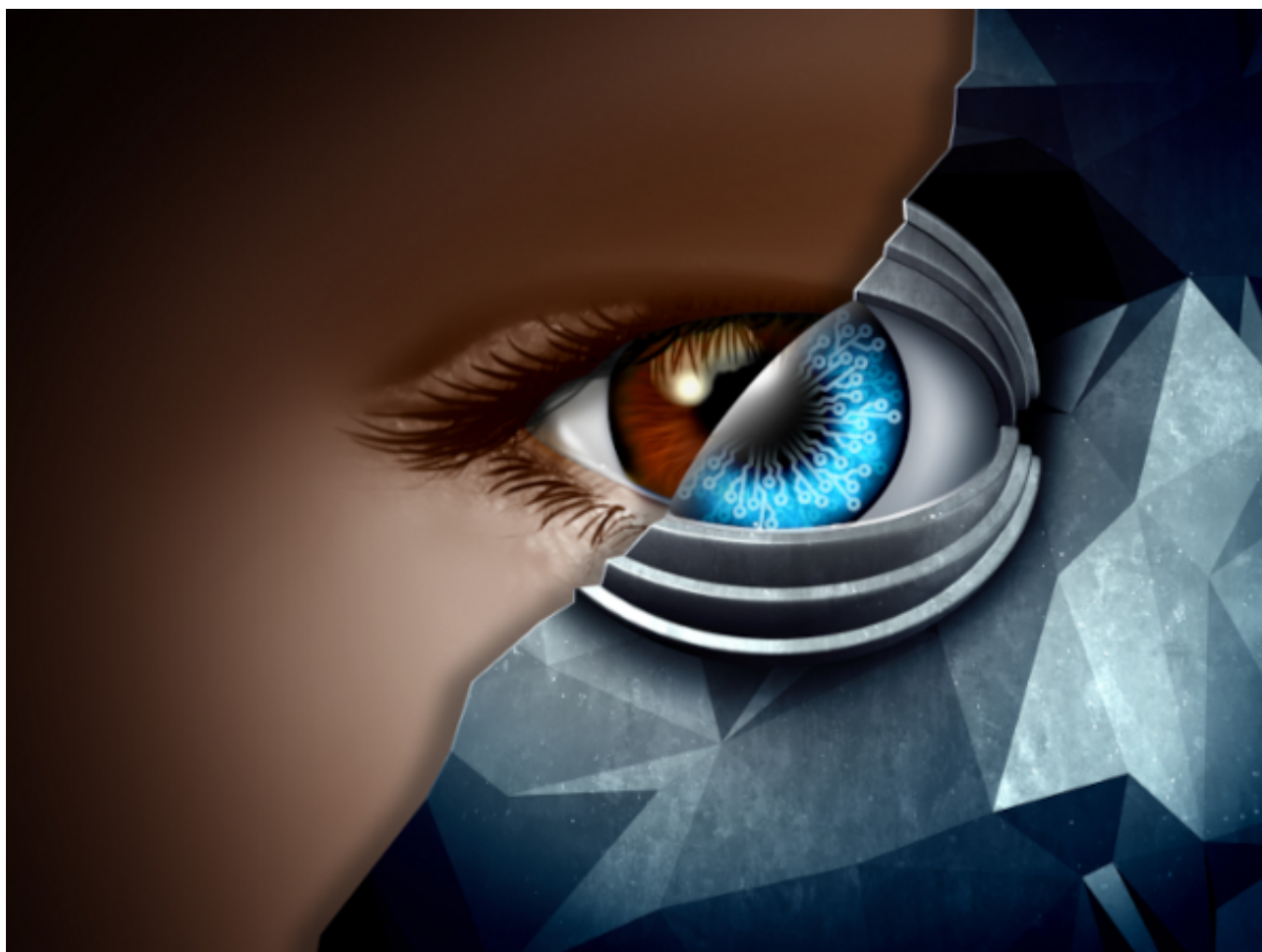
Figure 1:

(557)—Perché un dettaglio tecnico delle false IA sarà decisivo per cambiarne forse il modello di sviluppo, ma certamente quello di business?

9 novembre 2023— Cassandra ha da sempre sostenuto, come i 24 inscalfibili lettori ricorderanno bene, una posizione estremamente critica sulle attuali false Intelligenze Artificiali, cioè sui grandi modelli linguistici che vengono costantemente abusati per motivi commerciali.

Il problema delle false IA attuali non è quello di funzionare male; in effetti funzionano molto bene, se usate per fare quello per cui sono nate, cioè elaborare testi, come correttori ortografici "*on steroid*" quali effettivamente sono.

Il problema è piuttosto la campagna di marketing, globale e senza pari nella storia, con cui i modelli linguistici sono stati trasformati in occasioni di business, senza nessuna considerazione sui vantaggi e sui costi sociali che questo comporterà.

Senza nessuno scrupolo, insomma. Un film già visto e rivisto, purtroppo.

Quindi, tanto per cambiare e non annoiare troppo, Cassandra oggi racconterà un fatto tecnico poco noto sui modelli linguistici, che mette addirittura in dubbio il modello di marketing delle false Intelligenze Artificiali, e che questo marketing di rapina possa durare a lungo.

Il titolo di questa elucubrazione infatti, non è la solita iperbole, ma il nome di un fenomeno scientifico e dimostrato.

E, come spesso accade, per raccontare un argomento tecnico sono necessarie alcune premesse. Lettore avvertito ...

Nella *data economy* è indispensabile, per poter fare ricerca e sviluppo, utilizzare basi di dati "*di test*". Questo una volta non creava problemi; si prendevano, anzi *predavano* i primi dati "*veri*" che capitavano e li si usava. Poi li si pubblicava, magari cedendoli ad altri ricercatori e così via.

Tutto bene, apparentemente, ma cosa succedeva se si faceva ricerca medica? O sociologica? Od altri tipi di ricerca che dovessero trattare dati medici, genetici, od altri dati sensibili e particolari? Succedeva che dati critici, oggi abbastanza ben difesi dal GDPR e da altre norme, venissero elaborati, condivisi, diffusi e rielaborati al di fuori di ogni controllo.

Lo stessa trascuratezza già accaduta nei primi laboratori nucleari per la ricerca militare, in cui gli addetti ai lavori trasportavano radioisotopi in buste di plastica, magari tenute in tasca. D'altra parte anche il corpo di Maria Curie si trova in una bara di piombo, ed i suoi diari devo essere conservati sotto schermi antiradiazioni. La ricerca ha sempre esposto a rischi i primi scopritori, e magari anche altre persone, fa parte delle regole del gioco.

Tornando al nostro problema, la ricerca "*allegra*" dei *data scientist* ha esposto, non loro ma le persone i cui dati venivano usati, ad una nuova specie di rischio; la perdita e l'abuso dei propri dati particolari, medici, genetici, etc.

Grazie anche al GDPR sono poi stati presi provvedimenti, ma il problema di base era che i dati per la ricerca erano, sono e saranno sempre indispensabili. Che fare allora?

I ricercatori del settore hanno cominciato ad utilizzare nuove tecniche di *anonimizzazione* dei dati, molto sbandierate come soluzione, ma che in realtà si sono domostrate molto deboli, visto che altri ricercatori hanno sviluppato, con relativa facilità, tecniche di deanonimizzazione e reidentificazione dei dati che funzionavano benissimo. Come nota a margine, non a caso nel 2010 la deanonimizzazione è stato il tema principale di numerosi convegni, incluso e-privacy che descriveva il suo tema così:

... recenti progressi nelle tecniche di incrocio di dati personali, ben riassunte nella fondamentale ricerca di Paul Ohm "Broken promises of privacy: responding to the surprising failure of anonymization" hanno non scosso ma abbattuto completamente l'edificio tecnico-normativo della 196/2003, migrato però in parte anche nel GDPR, che considera l'anonimizzazione la più sofisticata barriera eretta a difesa dei dati personali e sensibili."

Per poter quindi usare dati "*realistici*", indispensabili per la ricerca, chi doveva trovare a tutti i costi una soluzione partorì una delle più grandi *supercazzole* scientifiche mai concepite, i "*dati sintetici*", cioè dati *realistici*, creati tramite metodi informatici. E' chiaro a tutti, tranne che agli specialisti, che nei dati sintetici, come nell'*appartamento spagnolo*, uno trova solo quello che porta. E se son dati, c'è solo l'informazione che ci si mette, non altro, non altre informazioni che possano essere estratte, come avviene per dati *veri*.

Le premesse, per i *fottuti eroi* che sono arrivati a leggere fin qui (come direbbe la "*Regina Rossa*"), sono finalmente terminate.

Torniamo quindi al tema di oggi, il collasso delle false Intelligenze Artificiali.

Alcuni fenomeni presentatisi durante l'attuale "*corsa*" alla creazione di modelli per IA, fenomeni che definire "*strani*" è poco, hanno portato a delle attività di ricerca e dei risultati decisamente interessanti.

In certi casi, ad esempio, continuare ad addestrare un modello di IA con sempre più dati provoca, in maniera controintuitiva, un peggioramento delle sue prestazioni. In termini semplici, il modello tende a dare risposte stereotipate, ad esempio sempre più simili alla domanda o sempre più simili tra loro. Il modello "***collassa***", diventa inutilizzabile.

Ora tenetevi forte, perché è stato dimostrato che questo avviene quando, volutamente o per sbaglio, il modello viene addestrato con dati sintetici.

Dare in pasto dati sintetici ad un modello di IA lo fa "disimparare".

"*Garbage in, garbage out*" direbbero gli anglofoni. Il conte Mascetti sintetizzerebbe meglio dicendo "*Se ascolti solo supercazzole, dirai solo supercazzole*".

Ed ora certamente qualcuno avrà pensato:

"*Che problema c'è, quindi? Non date in pasto dati sintetici alle IA e tutto si sistemerà.*"

Giusto, ma difficile a farsi. I dati sintetici sono simili ai dati reali, non è facile riconoscerli. E spuntano fuori dove meno te l'aspetteresti.

Tenetevi di nuovo forte. **Tutti i prodotti delle false IA, inclusi quei falsi articoli , news ed annunci, ma anche racconti, romanzi e pubblicazioni accademiche, sono in tutto od in parte dati sintetici**, e producono esattamente gli stessi problemi quando usati per addestrare una modello linguistico.

Una possibile ed interessante conseguenza di questo fenomeno è che l'inquinamento della Cultura e dell'Infosfera, causato dall'inserimento dei prodotti delle false intelligenze artificiali, potrebbe essere per loro stesse fatale, quando fossero *nutrite* con essi.

E' possibile sperare che gli esseri umani siano più resistenti a questo tipo di inquinamento rispetto alle false intelligenze artificiali. Queste comunque non potranno più essere addestrate semplicemente nutrendole in maniera indiscriminata con tutto quello che viene pubblicato sulla Rete.

Qualcuno dei 24 increduli lettori potrebbe ora pensare:

"*Ma allora basterà stringere i denti ed aspettare, e prima o poi le IA si estingueranno da sole*".

Magari! No, purtroppo, chi può dire come si comporteranno nuovi tipi di IA che verranno scoperti in futuro?

Però almeno il modello di sviluppo attuale delle false intelligenze artificiali, in cui gli OGAFAM prendono gratis tutta la cultura del mondo e la rivendono poi sotto forma di un loro prodotto esclusivo (le false Intelligenze Artificiali, appunto) non potrà durare.

In attesa quindi che qualcosa di nuovo emerga, magari fra 50 anni, nel campo dell'IA, gli OGAFAM dovranno cominciare a pagare per quello che usano, costretti a discriminare oculatamente per scegliere dati utili ed utilizzabili, e non dati sintetici o prodotti dalla false IA, e quindi "velenosi" per le stesse.

Come, purtroppo, sono "tossici" per noi e per la Cultura tutta.